First Hit Fwd Refs

Previous Doc

Next Doc

to Doc#

9/182279

etroni

Generate Collection

Print

L3: Entry 1 of 7

File: USPT

Nov 21, 2000

DOCUMENT-IDENTIFIER: US 6150921 A TITLE: Article tracking system

<u>Application Filing Date</u> (1): 19971017

<u>Detailed Description Text</u> (78):

Alternative tag designs enable variation in transmission time based on environmental factors. For example, motion detectors may be placed in a tag to decrease the time between transmissions when the tag is im motion. As another example, a tag might transmit more frequently and with higher power when the tag has been tampered with. As another example, a tag might incorporate a slightly modified Electronic Article Surveillance (EAS) device, which would cause the tag to transmit its UID more frequently when in range of a standard EAS detector. More generally, if a tag is attached to another electronic device, transmission interval can be modified under the control of that device.

Detailed Description Text (81):

For some situations, battery replacement may be accomplished by incorporating the battery in an attachment mechanism. For example, re-usable tag electronics may be attached to a disposable patient bracelet, with the battery included in the bracelet. As another example, a battery may be incorporated into the clip of an ID bracelet. More generally, a battery may be incorporated into an inexpensive disposable portion of an active RFID tag, with the electronics in the other, more expensive, portion.

Current US Cross Reference Classification (1):
340/5.8

Previous Doc

Next Doc

Go to Doc#

First Hit Fwd Refs Previous Doc Next Doc Go to Doc#

Generate Collection Print

L3: Entry 1 of 7 File: USPT Nov 21, 2000

US-PAT-NO: 6150921

DOCUMENT-IDENTIFIER: US 6150921 A

TITLE: Article tracking system

DATE-ISSUED: November 21, 2000

INVENTOR-INFORMATION:

NAME CITY STATE ZIP CODE COUNTRY

Werb; Jay Newton MA
Lanzl; Colin Nashua NH
McKinney; Kenelm Melrose MA

ASSIGNEE-INFORMATION:

NAME CITY STATE ZIP CODE COUNTRY TYPE CODE

PinPoint Corporation Billerica MA 02

APPL-NO: 08/ 953755 [PALM]
DATE FILED: October 17, 1997

PARENT-CASE:

REFERENCES TO RELATED APPLICATIONS This application claims priority from a provisional application Ser. No. 60/028,658, filed Oct. 17, 1996, a provisional application Ser. No. 60/044,321, filed Apr. 24, 1997, and a provisional application Ser. No. 60/044,245, filed Apr. 24, 1997.

INT-CL:  $[07] \underline{H04} \underline{Q} \underline{5/22}$ 

US-CL-ISSUED: 340/10.1; 340/825.34, 340/825.49, 340/573.1, 340/573.4, 342/42,

342/44

US-CL-CURRENT: 340/10.1; 340/5.8, 340/573.1, 340/573.4, 340/825.49, 342/42, 342/44

FIELD-OF-SEARCH: 340/825.54, 340/825.34, 340/825.49, 340/573.1, 340/573.4,

340/10.1, 342/42, 342/44

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected Search ALL Clear

PAT-NO ISSUE-DATE PATENTEE-NAME US-CL

31375 February 1861 Dodsworth

☐ 3098971 July 1963 Richardson

3273146	September 1966	Hurwitz, Jr.
3289114	November 1966	Rowen
3478344	November 1969	Schwitzgebel et al.
3706094	December 1972	Cole et al.
3707711	December 1972	Cole et al.
3740742	June 1973	Thompson et al.
3805264	April 1974	Lester
3914762	October 1975	Klensch
3944928	March 1976	Augenblick et al.
3964024	June 1976	Hutton et al.
3973200	August 1976	Akerberg
4019181	April 1977	Olsson et al.
4075632	February 1978	Baldwin et al.
4114151	September 1978	Denne et al.
4314373	February 1982	Sellers
4347501	August 1982	Akerberg
4364043	December 1982	Cole et al.
4399437	August 1983	Falck et al.
4459474	July 1984	Walton
4471345	September 1984	Barrett, Jr.
4481428	November 1984	Charlot, Jr.
4494119	January 1985	Wimbush
4495496	January 1985	Miller, III
4549169	October 1985	Moura et al.
4549264	October 1985	Carroll et al.
4598275	July 1986	Ross et al.
4605929	August 1986	Skeie
4613864	September 1986	Hofgen
4625207	November 1986	Skeie
4636950	January 1987	Caswell et al.
4651156	March 1987	Martinez
4656463	April 1987	Anders et al.
4658357	April 1987	Carroll et al.
4691202	September 1987	Denne
4703327	October 1987	Rossetti et al.
4724427	February 1988	Carroll
4725841	February 1988	Nysen et al.
4746830	May 1988	Holland

<u>4757315</u>	July 1988	Lichtenberg et al.	
4777478	October 1988	Hirsch et al.	
4786907	November 1988	Koelle	
4799062	January 1989	Sanderford, Jr. et al.	
4814751	March 1989	Hawkins et al.	
4818855	April 1989	Mongeon et al.	
4818998	April 1989	Apsell et al.	342/44
4819267	April 1989	Cargile et al.	
4862176	August 1989	Voles	
4888473	December 1989	Rossi et al.	
4888692	December 1989	Gupta et al.	
4897661	January 1990	Hiraiwa	
4918423	April 1990	Fukuyama et al.	
4918425	April 1990	Greenberg et al.	
4918493	April 1990	Geissberger et al.	
4924211	May 1990	Davies	
4952913	August 1990	Pauley et al.	
5025492	June 1991	Viereck	
5053774	October 1991	Schuermann et al.	
5062151	October 1991	Shipley	
5073781	December 1991	Stickelbrocks	
5095240	March 1992	Nysen et al.	
5099227	March 1992	Geiszler et al.	
5119104	June 1992	Heller	
5126746	June 1992	Gritton	
5144313	September 1992	Kirknes	
5163004	November 1992	Rentz	
5164985	November 1992	Nysen et al.	
<u>5194860</u>	March 1993	Jones et al.	
<u>5208756</u>	May 1993	Song	
5216612	June 1993	Cornett et al.	
5218344	June 1993	Ricketts	
5221831	June 1993	Geiszler	
5222099	June 1993	Hori et al.	
5224034	June 1993	Katz et al.	
5249120	September 1993	Foley	
5252979	October 1993	Nysen	

	•		
5262784	November 1993	Drobnicki et al.	
5276496	January 1994	Heller et al.	
5287112	February 1994	Schuermann	
5289372	February 1994	Guthrie et al.	
5294931	March 1994	Meier	
5311185	May 1994	Hochstein et al.	
5311438	May 1994	Sellers et al.	
5311562	May 1994	Palusamy et al.	
5317309	May 1994	Vercellotti et al.	
5321605	June 1994	Chapman et al.	
5331545	July 1994	Yajima et al.	
5343387	August 1994	Honma et al.	
5355137	October 1994	Schurmann	
5359250	October 1994	Toda	
5359322	October 1994	Murray	
5365516	November 1994	Jandrell	
5369570	November 1994	Parad	
5382784	January 1995	Eberhardt	
5424746	June 1995	Schwab et al.	
5426284	June 1995	Doyle	
5428547	June 1995	Ikeda	
5430889	July 1995	Hulbert et al.	
5440301	August 1995	Evans	
5448221	September 1995	Weller	
5450492	September 1995	Hook et al.	
5455409	October 1995	Smith et al.	
5455851	October 1995	Chaco et al.	
5467268	November 1995	Sisley et al.	
5469170	November 1995	Mariani	
5471404	November 1995	Mazer	
5477225	December 1995	Young et al.	
5499071	March 1996	Wakabayashi et al.	
5504936	April 1996	Lee	
5506584	April 1996	Boles	
5506864	April 1996	Schilling	
5517194	May 1996	Carroll et al.	340/825.54
5521602	May 1996	Carroll et al.	

	5526357	June 1996		Jandrell		
	5528232	June 1996		Verma et al.		
	5539394	July 1996		Cato et al.		340/825.34
	5539775	July 1996		Tuttle et al.		
	5550547	August 1996		Chan et al.		
	5552772	September 1996	6	Janky et al.		
	5552790	September 1996	6	Gunnarsson		
	5565858	October 1996		Guthrie		
	5581486	December 1996		Terada et al.		
	5586057	December 1996		Patel		
	5592180	January 1997		Yokev et al.		
	5596507	January 1997		Jones et al.		
	5602538	February 1997		Orthmann et al.		340/825.54
	5608621	March 1997		Caveney et al.		
	5617342	April 1997		Elazouni		
	5621411	April 1997		Hagl et al.		
	5621412	April 1997		Sharpe et al.		340/825.54
	5623413	April 1997		Matheson et al.		
	5630070	May 1997		Dietrich et al.		
	5640151	June 1997		Reis et al.		
	5663956	September 1997	7	Schilling		
	5678186	October 1997		Lee		
	<u>5710566</u>	January 1998		Grabow et al.		340/825.54
	5714932	February 1998		Castellon et al.		
	5722059	February 1998		Campana, Jr.		
	<u>5726630</u>	March 1998		Marsh et al.		340/825.54
	<u>5731785</u>	March 1998		Lemelson et al.		
	5995017	November 1999		Marsh et al.		340/825.34
			FORE	EIGN PATENT DOCUMENT	rs	
	EIGN-PAT-N	0	PUBN-		COUNTRY	US-CL
	89 325 A1 67 036 A2		March June		EP EP	
	34 140			ry 1991	GB	
2 2	46 891			ary 1992	GB	
	92/17947		Octob	er 1992	WO	
WO	96/18913		June	1996	WO	

#### OTHER PUBLICATIONS

Takeshi Manabe, IEEE Transactions on Atenna and Propagation 40(5):500-509 (1992). Ollivier, RFID-A Practical Solution for Problems You Didn't Even Know You Had!, Texas Instruments Ltd., The Institution of Electrical Engineering, London, UK, (1996).

Williamson et al., IEEE, pp. 186-201 (1993).

Plessky et al., IEEE pp. 117-120 (1995).

Standard Dictionary of Electrical and Electronics Terms, An American National Standard, Fourth Edition pp. 663-1040 (1988).

Hurst, "Quiktrak: A Unique New AVL System", Proceedings of the Vehicle Navigation and Information Systems Conference, Toronto, pp. A60-A62 (1989).

Internet reference address http://www.tagmaster.se/products/index.htm, TagMaster Mark Tag.TM. S1255.

ART-UNIT: 275

PRIMARY-EXAMINER: Horabik; Michael

ASSISTANT-EXAMINER: Dalencourt; Yves

ATTY-AGENT-FIRM: Hutchins, Wheeler & Dittmar

#### ABSTRACT:

System for tracking mobile tags. Cell controllers with multiple antenna modules generate a carrier signal which is received by the tags. Tags shift the frequency of the carrier signal, modulate an identification code onto it, and transmit the resulting tag signal at randomized intervals. The antennas receive and process the response, and determine the presence of the tags by proximity and triangulation. Distance of a tag from an antenna is calculated by measuring the round trip signal time. The cell controllers send data from the antenna to a host computer. The host computer collects the data and resolves them into positional estimates. Data are archived in a data warehouse, such as an SQL Server.

38 Claims, 23 Drawing figures

Previous Doc Next Doc Go to Doc#



# Refine Search

# Search Results -

Terms	Documents
L5 and (authentic\$ or verif\$)	3

US Pre-Grant Publication Full-Text Database
US Patents Full-Text Database

Database:

US OCR Full-Text Database EPO Abstracts Database JPO Abstracts Database Derwent World Patents Index IBM Technical Disclosure Bulletins

Search:

7	333
	***************************************
<u> </u>	3

Refine Search

Re	ecall	Text	<b>-</b>

Clear

Interrupt

# **Search History**

# DATE: Wednesday, December 01, 2004 Printable Copy Create Case

Set Name side by side	Query	<u>Hit</u> <u>Count</u>	Set Name result set
DB=U	SPT; THES=ASSIGNEE; PLUR=YES; OP=OR		
<u>L7</u>	L5 and (authentic\$ or verif\$)	3	<u>L7</u>
<u>L6</u>	L5 and (authentic\$ and verif\$)	3	<u>L6</u>
<u>L5</u>	L4 and l2	7	<u>L5</u>
<u>L4</u>	((electronic\$ with tag) same (product or goods or item)) and @ad<=19981029	243	<u>L4</u>
<u>L3</u>	L2 and l1	4	<u>L3</u>
<u>L2</u>	705/26;340/5.8.ccls.	1314	<u>L2</u>
<u>L1</u>	((electronic\$ near2 tag) same (product or goods or item)) and @ad<=19981029	109	<u>L1</u>

# **END OF SEARCH HISTORY**



# Refine Search

# Search Results -

Terms	Documents
L4 and L2	7

US Pre-Grant Publication Full-Text Database
US Patents Full-Text Database
US OCR Full-Text Database
EPO Abstracts Database
JPO Abstracts Database
Derwent World Patents Index
IBM Technical Disclosure Bulletins

Search:

ı	L5		
I		***************************************	Refine Search
ļ		<u> </u>	
	Recall Text 🚓		Interrupt
	INCOMI TOAL		

# **Search History**

# DATE: Wednesday, December 01, 2004 Printable Copy Create Case

Set Name side by side	Query	<u>Hit</u> Count	<u>Set</u> <u>Name</u> result set
DB=U	SPT; THES=ASSIGNEE; PLUR=YES; OP=OR		
<u>L5</u>	L4 and l2	7	<u>L5</u>
<u>L4</u>	((electronic\$ with tag) same (product or goods or item)) and @ad<=19981029	243	<u>L4</u>
<u>L3</u>	L2 and 11	4	<u>L3</u>
<u>L2</u>	705/26;340/5.8.ccls.	1314	<u>L2</u>
<u>L1</u>	((electronic\$ near2 tag) same (product or goods or item)) and @ad<=19981029	109	<u>L1</u>

# **END OF SEARCH HISTORY**

# **Hit List**

Clear Generate Collection Print Fwd Refs Bkwd Refs
Generate OACS

**Search Results -** Record(s) 1 through 7 of 7 returned.

☐ 1. Document ID: US 6535108 B1

L5: Entry 1 of 7

File: USPT

Mar 18, 2003

US-PAT-NO: 6535108

DOCUMENT-IDENTIFIER: US 6535108 B1

TITLE: Modulation of the resonant frequency of a circuit using an energy field

Full Title Citation Front Review Classification Date Reference Claims KMC Draw. Co.

2. Document ID: US 6167568 A
L5: Entry 2 of 7 File: USPT Dec 26, 2000

US-PAT-NO: 6167568

DOCUMENT-IDENTIFIER: US 6167568 A

TITLE: Method and apparatus for implementing electronic software distribution

Full Title Citation Front Review Classification Date Reference Classification Date Classification Date Reference Classification Date Cla

File: USPT

US-PAT-NO: 6144301

L5: Entry 3 of 7

DOCUMENT-IDENTIFIER: US 6144301 A

TITLE: Electronic tracking tag

Full | Title | Citation | Front | Review | Classification | Date | Reference | Residence |

4. Document 1D. 05 3702071 7

L5: Entry 4 of 7

File: USPT

Nov 9, 1999

Nov 7, 2000

US-PAT-NO: 5982891

DOCUMENT-IDENTIFIER: US 5982891 A

TITLE: Systems and methods for secure transaction management and electronic rights

protection

Full Title Citation Front Review	Classification Date Reference	Claims KWC Draw D
☐ 5. Document ID: US 5	915019 A	
L5: Entry 5 of 7	File: USPT	Jun 22, 1999
US-PAT-NO: 5915019 DOCUMENT-IDENTIFIER: US 5915	019 A	
TITLE: Systems and methods f protection	or secure transaction manageme	nt and electronic rights
Full   Title   Citation   Front   Review	Classification Date Reference	Claims KMC Draw.D
☐ 6. Document ID: US 5	873069 A	
L5: Entry 6 of 7	File: USPT	Feb 16, 1999
US-PAT-NO: 5873069 DOCUMENT-IDENTIFIER: US 5873	069 A	
TITLE: System and method for	automatic updating and displa	y of retail prices
Full Title Citation Front Review	Classification Date Reference	Claims KWC Draw. D
***************************************		
☐ 7. Document ID: US 5		
L5: Entry 7 of 7	File: USPT	May 26, 1998
US-PAT-NO: 5757521 DOCUMENT-IDENTIFIER: US 5757	521 A	
TITLE: Pattern metallized op	tical varying security devices	
Full Title Citation Front Review	)   Classification   Date   Reference	SELECTION Claims KAMC Draw, D
Clear Generate Collection	Print Fwd Refs Bkwc	Refs Generate OACS
Terms L4 and L2	Documents	7
<u>Displa</u>	y Format: TI Change Format	

# First Hit Fwd Refs Previous Doc Next Doc Go to Doc# End of Result Set Generate Collection Print

L6: Entry 3 of 3 File: USPT May 26, 1998

DOCUMENT-IDENTIFIER: US 5757521 A

TITLE: Pattern metallized optical varying security devices

# Application Filing Date (1): 19951121

#### Brief Summary Text (2):

The present invention generally relates to <u>authenticating</u> devices, and more particularly relates to holograms used as security and anti-counterfeiting components of personal identification cards, credit cards, product labels, documents, currency and the like.

#### Brief Summary Text (4):

Holograms are commonly used as <u>authenticating</u> devices since the hologram, providing a three-dimensional image, is difficult to copy or reproduce. Holograms are records of an interference pattern formed by light at a recording location. Typically a photographic plate, placed at the recording location, is used to make and preserve an original holographic record. Commonly, the recorded interference pattern is that of a three dimensional image of a subject.

## Brief Summary Text (12):

Various credit and identification cards, as well as some product labels, employ commercial holograms or diffraction gratings to deter counterfeiting by providing a visual indication of <u>authenticity</u>. Some product labels and currency depend on fine plastic threads with metallic print to increase the difficulty of counterfeiting, also by providing a visual indication of <u>authenticity</u>. Both holograms and fine metallic print are used together in these and other applications, because the visual indication of <u>authenticity</u> is both difficult to reproduce by conventional means and easily <u>verified</u> by direct observation. For further security, the hologram or metal printing security device may be secured to the document such that the security device will be destroyed or otherwise exhibit evidence of tampering upon any attempt to remove the security device. This will be discussed in further detail below.

#### Brief Summary Text (25):

Finally, current security devices generally require visual inspection, possibly with the aid of special equipment to verify authenticity. Quick, automatic security scanners currently require additional features to be incorporated into identification cards, product labels, and the like. Such features may include bar codes, microwave resonant structures, and various other electrically or optically detectable features which may be remotely sensed. Adding these features to identification cards, product labels and the like complicates the production of the objects or documents to which the security devices have been attached.

#### Brief Summary Text (30):

A method of <u>authenticating</u> an article forms a third aspect of the invention. The method may comprise the steps of: adhering to the article a surface relief hologram; disposing a metal pattern between the surface relief hologram and the

Record Display Form Page 2 of 6

article; illuminating the metal pattern with electromagnetic energy swept over a predetermined frequency range and at a predetermined rate; and analyzing reradiated electromagnetic energy to authenticate the article. The method of this aspect of the invention may by modified in that the step of analyzing may further comprise the step of comparing a spectrum of the re-radiated electromagnetic energy to an expected spectral signature of the metal pattern.

# Brief Summary Text (31):

A method of authenticating an article according to a fourth aspect of the invention may comprise the steps of: adhering to the article a surface relief hologram; disposing a metal pattern between the surface relief hologram and the article; measuring a plurality of reflection coefficients of the metal pattern at a corresponding plurality of frequencies; and comparing each reflection coefficient with an expected reflection coefficient at a corresponding frequency.

#### Brief Summary Text (32):

In accordance with a fifth aspect of the invention, there is provided a method of authenticating an article, which may comprise the steps of: adhering to the article a device including a surface relief hologram; disposing a metal pattern between the surface relief hologram and the article; measuring capacitance of the metal pattern; and comparing the capacitance measured with an expected capacitance. Also in accordance with this aspect of the invention, authentication may be deactivated by performing the steps of: forming the metal pattern of a plurality of areas connected by a fusible link; and generating an electric current between the plurality of areas, thereby causing the fusible link to break. Further in accordance with this aspect of the invention, the step of generating may further comprise any one of the steps of: (a) bringing an electric charge into proximity with the plurality of areas, (b) applying an electric field to the plurality of areas, and (c) applying a time-varying magnetic field to the plurality of areas.

# Detailed Description Text (12):

As shown in the example of FIG. 7B, the device of FIG. 7A may be enhanced by forming a high frequency, electromagnetically resonant structure 717 in the metallization layer. A series-resonant inductor 719 and capacitor 721a and 721b (LC) circuit, as shown, may operate in the 8-10 MHz range. The particular, precise frequency of resonance could serve as a code indicative of authenticity. In the illustrated structure, when the overlaminate is folded and applied to a document to be secured, the plates 721a and 721b act as a capacitor, with the secured document between them forming the dielectric. A coil 719 completes the resonant circuit. As in FIG. 7A, each identification card receives one or more full or random portions of the repeating pattern 711. The surface relief hologram of the overlaminate is enhanced by a continuous grid screen, as described above in connection with FIGS. 6A and 6B. Again, both the hologram and the underlying printed and pictorial information on the identification card are observable. Areas of the overlaminate which cover underlying identification information may be clear or may be metallized with a continuous grid screen to form a semi-transparent hologram. Areas of the overlaminate which do not cover any underlying identification information, for example those portions of the overlaminate corresponding to the back of the identification card, may be made opaque with a more complete metallization, metallized text or metallized graphics.

## Detailed Description Text (13):

The structure of FIG. 7C is again similar to that of FIGS. 7A and 7B. However, microwave frequency resonant structures 723, which operate in the GHz frequency ranges are formed in the metallization, rather than the high frequency LC resonant circuit 717. The microwave frequency resonant structures 723 are simply metallized areas of shapes computed to exhibit desired resonances. In this type of structure, the particular combination of resonant frequencies serves as a code indicative of authenticity.

Record Display Form Page 3 of 6

## Detailed Description Text (25):

Employing elements from those aspects of the invention and methods discussed above, a new and useful security device may be made as shown in exploded view in FIG. 10. Authentication by both overt and covert means is achieved by this new device.

#### <u>Detailed Description Text</u> (27):

The metallic pattern 1001 shown amplifies the surface relief hologram 1005, as discussed above with respect to other embodiments of the invention. Also as discussed above, the metallic pattern 1001 may be of the continuous grid type, which is conductive, yet not opaque. A layer of about 200 .ANG. of Al with a protective layer of about 25 .ANG. of AlO.sub.2 is preferred. The thickness of the metallic pattern layer and the protection layer may be varied by one of ordinary skill in this art to achieve different levels of transparency, oxidation protection and other parameters as required. The item to which the device may be applied may thus be viewed through the surface relief hologram 1005 on which the metallic pattern 1001 has been applied. However, the illustrated device is difficult for a counterfeiter to reproduce, because the precise registration between the surface relief hologram 1005 and the metallic pattern 1001 is difficult to reproduce. The amplified surface relief hologram (1005 combined with 1001) provides an overt indication of authenticity, in that it is optically detectible, readily verifiable by human observation, and yet difficult to reproduce. The overt indicia of authenticity could also include metallization micro-printing 1002, which may be readily detected with modest magnification, but which is exceedingly difficult to reproduce. The characters of micro-printing 1002 may be 0.025" high, for example.

#### Detailed Description Text (28):

In addition to the overt indication of authenticity provided by the device, there may be provided covert indications of authenticity. For example, the metallic pattern 1001 may form one or more resonators or antennae, which when illuminated by electromagnetic energy swept through a predetermined frequency range at a predetermined rate of frequency change, radiated by a transceiver 1007, re-radiates that electromagnetic energy resonating at one or more predetermined frequencies. The re-radiated energy may be detected by a receiver section of the transceiver 1007, in which the received spectrum is compared with the pattern produced by a valid device. The receiver could perform a spectrum analysis over a frequency range of interest. The spectral signature of a valid device is then compared with the spectrum of the received energy. A decision regarding the authenticity of the device may then be made based on the comparison.

#### Detailed Description Text (29):

Devices may be produced which provide similar or indistinguishable overt indicia of authenticity, but which encode different covert indicia, by varying the millimeter resonators included in metallic pattern 1001. Furthermore, additional, transparent conductors may be connected to the metallic pattern 1001, altering the electrical characteristics of the device, but visually non-detectible. Since a wide variety of codes could thus be produced, the device could be used, for example, to identify goods intended for different market channels, to identify goods manufactured at different plants, or to identify goods manufactured or shipped at different times, etc. Those skilled in the art would be able to identify numerous types of useful information which could be encoded in the spectral characteristics of the metallic pattern 1001.

## Detailed Description Text (30):

A second electromagnetic characteristic of a patterned metallic holographic label which may be used to electronically authenticate a patterned metallized holographic tag or label is the metallic pattern's inherent impedance. Impedance is taken to refer to a complex impedance having both a magnitude and a phase. A complex quantity is required to describe a structure's impedance because the structure may include both resistance and reactance. A structure's impedance, of course, is a function of frequency. Furthermore, it is well known that network analyzers

determine a structure's impedance as a function of frequency by measuring the structure's reflection coefficient as a function of frequency. Like impedance, the reflection coefficient of a structure is taken to be a complex quantity represented by a magnitude and a phase because the structure may have both resistance and reactance. Knowing the reflection coefficient at a given frequency, impedance at the given frequency is readily calculated. Measured at several frequencies, a structure's reflection coefficients characterize and parameterize a structure including conductive, magnetic and dielectric components to such a degree that the reflection coefficients can be used to authenticate a patterned metallized holographic security tag or label with a reasonable degree of certainty. As the reflection coefficient is 1) directly related to the tag's impedance at the measurement frequency, and 2) a function of both the metallic pattern and component substrates, it represents a measurable, identifiable, authenticating electromagnetic signature.

#### Detailed Description Text (31):

A hand held device 1007, having the capability to generate and radiate up to four frequencies, for example, which functions similarly to a network analyzer can measure and store the four reflection coefficients of an <u>authentication</u> label 1015. The hand-held, miniature, network analyzer 1007 emits four low-level microwave signals which are reflected by the patterned metallized security tag or label 1015, the reflected signals are compared to reference signals to produce the tag's reflection coefficients. These four reflection coefficients characterize the <u>authentication</u> tag 1015 and can be compared a valid tag's reflection coefficients in order to make an <u>authentication</u> decision. In order to function effectively the <u>authentication</u> device 1007 should be positively positioned with respect to the <u>authentication</u> label 1015. Direct contact would clearly positively position the <u>authentication</u> device and is one option. Repeatable results are ensured by providing a repeatable sensor-tag-sensor path length.

#### Detailed Description Text (32):

The impedance of the <u>authentication</u> device 1007 may be measured by other means. For example, an instrument such as the MDA-1000 microwave dielectric analyzer (KDC Technology Corporation; Acton, Mass.) could be readily adapted by one skilled in this art to determine the impedance of <u>authentication</u> device 1007. The MDA-1000 uses an open reflection microwave resonator driven by a low-level microwave signal which is stepped through a narrow band of frequencies covering the resonator's resonant frequency. Resonant frequency and return loss of the signal affected by the material under test are measured. Impedance may then be calculated therefrom. It will be understood by those skilled in this art that other measurement techniques are adaptable to the task of measuring the impedance of the <u>authentication</u> device 1007.

# Detailed Description Text (33):

A third authentication mechanism based on the electrical characteristics of a tag or label, measures the capacitance of a patterned metallized, holographic security tag with a custom designed, hand-held, bridge capacitance meter. FIG. 12 illustrates a simple probe 1201 which includes a plurality of capacitive plates 1204 of opposite polarities. The probe 1201 contacts the authentication tag 1202 in a predetermined position and the tag's capacitance is measured. The tag's capacitance is a function of 1) the thickness and dielectric constant of the polymeric film 1203 between the probe and the metallized pattern, and 2) the metallic area (FIG. 13, 1301) in closest proximity to the probe plates 1204. A connected metallized area 1302 shown in FIG. 13 is a contiguous metallic area which when projected onto the contacted surface of tag 1202, links at least part of the area contacted by two probe plates 1204 of opposite polarity. Furthermore, only that area 1301 of a connected area in immediate proximity to probe plate contributes significantly to the measured capacitance. Similar metallic patterns can have different capacitive signatures due to subtle metallic connections between a metallic areas making one a contiguous connected area and the other merely part

of a metallic camouflage. As subtle connections can make a contiquous metallized area a connected area and thus contribute to the measured capacitance, thin strips linking metallized areas under probe-plates can also function as fuses 1303. For example, when a fuse 1303 linking two larger areas, one underneath the one probeplate and the second under the other probe-plate, is intact, the connected area contributes to the measured capacitance. When the fuse link is broken, the metallized area is no longer a connected area and hence does not contribute appreciably to the measured capacitance. Simply by applying a large charge to the probe-plates of the same probe 1201 which measures the capacitance, or otherwise bringing an electric field sufficient to induce a fusing current into proximity with the device, the fuse link 1303 can be deliberately broken, changing the measured capacitance. Likewise, in this embodiment or the previously described embodiment involving re-radiation of electromagnetic energy, a fuse link may be broken by applying a time-varying magnetic field of sufficient strength to induce a fusing current. This allows authentication labels to be deactivated by the same device which authenticates the tag.

# Detailed Description Text (35):

There are two further measures, which would significantly increase the difficulty of counterfeiting a capacitor tag. One is to choose for this buried, hidden layer a conductive substance, such as zinc, which readily oxidizes when exposed to the atmosphere. A second is to use a transparent conductive material. Each of the readily oxidizable conductive substance or the transparent conductive substance could be used in combination with a more conventional metallic conductive material or with each other. A counterfeiter, in order to replicate a valid tag, must first examine a valid tag to determine its structure. During this examination the transparent conductive material may not be detected or the readily oxidizable conductive material may be exposed to atmosphere thus preventing the conductive layer's constituent material, location and or size being completely determined. A counterfeit tag made without precise and complete information concerning the buried conductive layer would, if measured, not indicate the same capacitance as a valid tag and consequently would not be authenticated.

#### Detailed Description Text (36):

Patterned metallized holographic security tags or labels which appear the same to the unaided eye but which have different underlying metallic patterns, each having a unique electromagnetic signature which can be detected and decoded, provide the basis of a product security system which provides two desirable ingredients: 1) a visual authentication component, i.e., the pattern metallized hologram; and 2) a covert authentication means. The intended country of retail or other information could be encoded in the pleason and gray aiding deterrence of grey marketing or providing other useful product tracking features. The device which authenticates the holographic security tag could-detect such encoded information about the product's place of manufacture or intended market.

Current US Cross Reference Classification (5): 340/5.8

#### CLAIMS:

9. A method of authenticating an article, comprising the steps of:

adhering to the article a surface relief hologram;

disposing a metal pattern on the surface relief hologram so as to amplify visibility of the surface relief hologram to an observer:

illuminating the metal pattern with electromagnetic energy swept over a predetermined frequency range and at a predetermined rate; and

analyzing re-radiated electromagnetic energy to authenticate the article.

11. A method of authenticating an article, comprising the steps of:

adhering to the article a surface relief hologram;

disposing a metal pattern on the surface relief hologram so as to amplify visibility of the surface relief hologram to an observer;

measuring a frequency-dependent parameter of the article; and

comparing the measured frequency-dependent parameter of the article to an expected frequency-dependent parameter of an authentic article.

14. A method of authenticating an article, comprising the steps of:

adhering to the article a device including a surface relief hologram;

disposing a metal pattern on the surface relief hologram so as to amplify visibility of the surface relief hologram to an observer, the metal pattern positional between the surface relief hologram and the article;

measuring capacitance of the metal pattern; and

comparing the capacitance measured with an expected capacitance.

15. The method of claim 14, further including deactivating authentication, further comprising the steps of:

forming the metal pattern of a plurality of areas connected by a fusible link; and

generating an electric current between the plurality of areas, thereby causing the fusible link to break.

> Previous Doc Next Doc Go to Doc#